* **BATCH ID: WiproNGA\_DWS\_B5\_25VID2550**
* **NAME:** Shrawani Shyam Balwadkar
* **RPS USER ID:** 34932
* **DATE**: 26-08-2025

**TOPIC:**

* **How to take Backup in SCCM.**
* **WSUS Clean-up task, office 365 Updates option and synchronization, Multiple ADR deployment.**
* **Steps to use software Metering in SCCM.**
* **What is Client Cache Setting in SCCM.**

**Manage settings for software updates**

**Client settings for software updates**

After you install the software update point, software updates is enabled on clients by default, and the settings on the **Software Updates** page in client settings have default values. The client settings are used site-wide and affect when software updates are scanned for compliance, and how and when software updates are installed on client computers. Before you deploy software updates, verify that the client settings are appropriate for software updates at your site.

**Configure a software update point to use TLS/SSL with a PKI certificate**

Configuring Windows Server Update Services (WSUS) servers and their corresponding software update points (SUP) to use TLS/SSL may reduce the ability of a potential attacker to remotely compromise a client and elevate privileges. To ensure that the best security protocols are in place, we highly recommend that you use the TLS/SSL protocol to help secure your software update infrastructure. This article walks you through the steps required to configure each of your WSUS servers and the software update point to use HTTPS. For more information about securing WSUS, see the [Secure WSUS with the Secure Sockets Layer Protocol](https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/2-configure-wsus#25-secure-wsus-with-the-secure-sockets-layer-protocol) article in the WSUS documentation

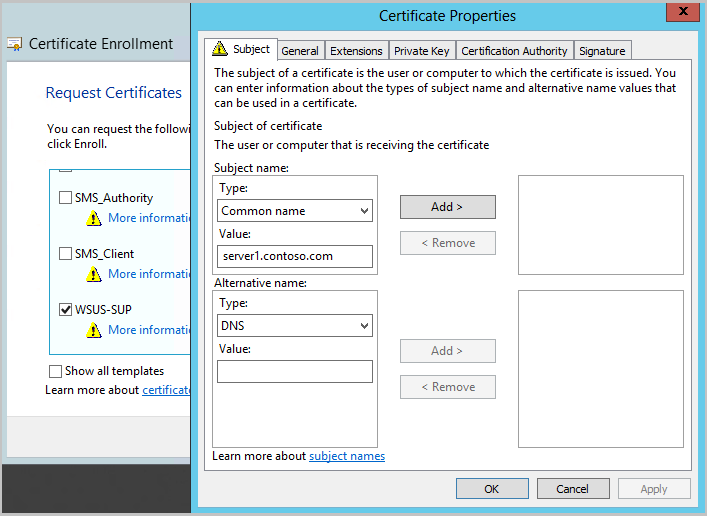
**Obtain the certificate from the CA if needed**

If you already have an appropriate certificate in the WSUS server's **Personal** certificate store, skip this section and start with the [Bind the certificate](https://learn.microsoft.com/en-us/intune/configmgr/sum/get-started/software-update-point-ssl#bkmk_bind) section. To send a certificate request to your internal CA to install a new certificate, follow the instructions in this section.

1. From the WSUS server, open an administrative command prompt and run certlm.msc. Your user account needs to be a local administrator to manage certificates for the local computer.

The Certificate Manager tool for the local device appears.

1. Expand **Personal**, then right-click on **Certificates**.
2. Select **All Tasks** then **Request New Certificate**.
3. Choose **Next** to begin certificate enrollment.
4. Choose the type of certificate to enroll. The certificate purpose is **Server Authentication** and the Microsoft certificate template to use is **Web Server** or a custom template that has **Server Authentication** specified as **Enhanced Key Usage**. You may be prompted for additional information to enroll the certificate. Typically, you'll specify the following information at minimum:
   * **Common name:** Found on the **Subject** tab, set the value to the WSUS server's FQDN.
   * **Friendly name:** Found on the **General** tab, set the value to a descriptive name to help you identify the certificate later.



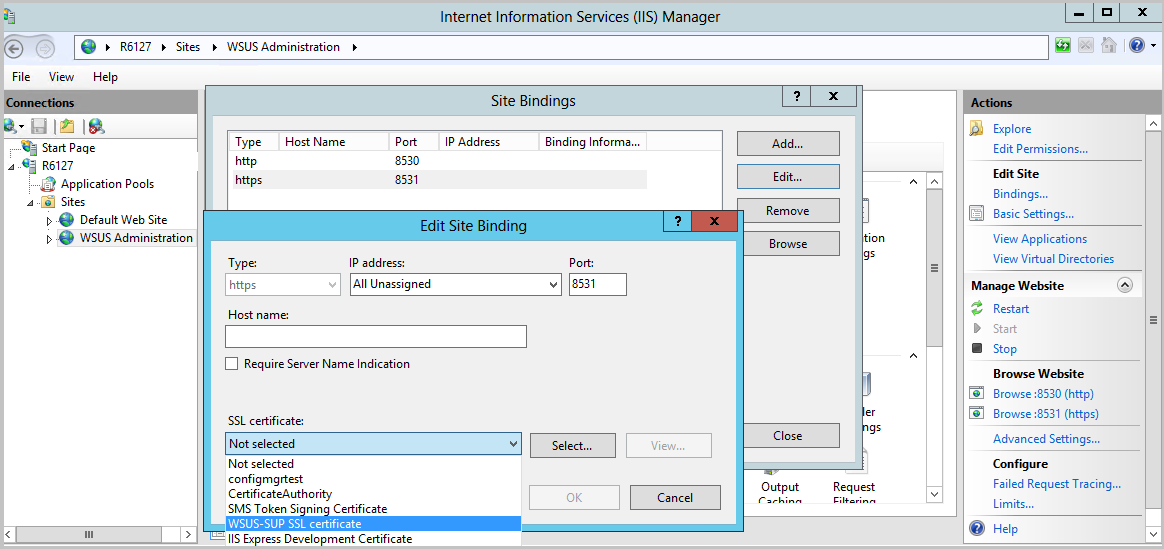
6.Select **Enroll** then **Finish** to complete the enrollment.

7.Open the certificate if you want to see details about it such as the certificate's thumbprint.

**Bind the certificate to the WSUS Administration site**

Once you have the certificate in the WSUS server's personal certificate store, bind it to the WSUS Administration site in IIS.

1. On the WSUS server, open Internet Information Services (IIS) Manager.
2. Go to **Sites** > **WSUS Administration**.
3. Select **Bindings** from either the action menu or by right-clicking on the site.
4. In the **Site Bindings** window, select the line for **https**, then select **Edit...**.
   * Don't remove the HTTP site binding. WSUS uses HTTP for the update content files.
5. Under the **SSL certificate** option, choose the certificate to bind to the WSUS Administration site. The certificate's friendly name is shown in the drop-down menu. If a friendly name wasn't specified, then the certificate's IssuedTo field is shown. If you're not sure which certificate to use, select **View** and verify the thumbprint matches the one you obtained.



1. Select **OK** when you're done, then **Close** to exit the site bindings. Keep Internet Information Services (IIS) Manager open for the next steps.

**Configure the WSUS web services to require SSL**

1. In IIS Manager on the WSUS server, go to **Sites** > **WSUS Administration**.
2. Expand the WSUS Administration site so you see the list of web services and virtual directories for WSUS.
3. For each of the below WSUS web services:
   * ApiRemoting30
   * ClientWebService
   * DSSAuthWebService
   * ServerSyncWebService
   * SimpleAuthWebService

Make the following changes:

* + Select **SSL Settings**.
  + Enable the **Require SSL** option.
  + Verify the **Client certificates** option is set to **Ignore**.
  + Select **Apply**.

Don't set the SSL settings at the top-level WSUS Administration site since certain functions, such as content, need to use HTTP.

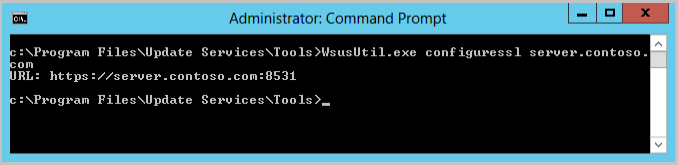
**Configure the WSUS application to use SSL**

Once the web services are set to require SSL, the WSUS application needs to be notified so it can do some additional configuration to support the change.

1. Open an admin command prompt on the WSUS server. The user account running this command must be a member of either the WSUS Administrators group or the local Administrators group.
2. Change directory to the tools folder for WSUS:

cd "c:\Program Files\Update Services\Tools"

1. Configure WSUS to use SSL with the following command:
2. WsusUtil returns the URL of the WSUS server with the port number specified at the end. The port will be either 8531 (default) or 443. Verify the URL returned is what you expected. If something was mistyped, you can run the command again.



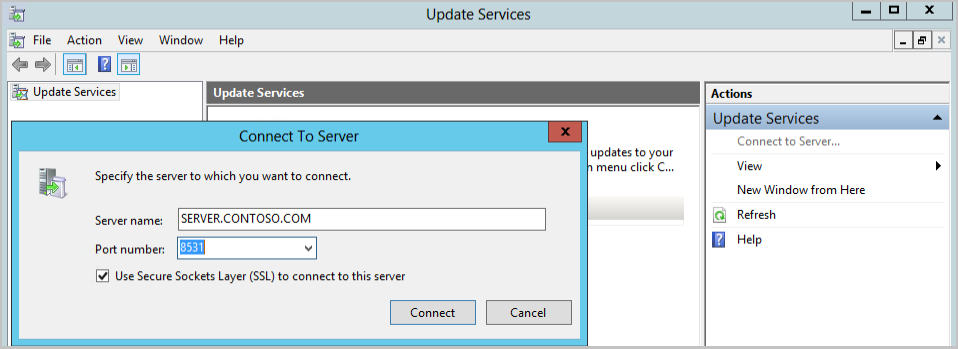
**Verify the WSUS console can connect using SSL**

The WSUS console uses the ApiRemoting30 web service for connection. The Configuration Manager software update point (SUP) also uses this same web service to direct WSUS to take certain actions such as:

* Initiating a software update synchronization
* Setting the proper upstream server for WSUS, which is dependent on where the SUP's site resides in your Configuration Manager hierarchy
* Adding or removing products and classifications for synchronization from the hierarchy's top-level WSUS server.
* Removing expired updates

Open the WSUS console to verify you can use an SSL connection to the WSUS server's ApiRemoting30 web service. We'll test some of the other web services later.

1. Open the WSUS console and select **Action** > **Connect to Server**.
2. Enter the FQDN of the WSUS server for the **Server name** option.
3. Choose the **Port number** returned in the URL from WSUSutil.
4. The **Use Secure Sockets Layer (SSL) to connect to this server** option automatically enables when either 8531 (default) or 443 are chosen.



1. If your Configuration Manager site server is remote from the software update point, launch the WSUS console from the site server and verify the WSUS console can connect over SSL.
   * If the remote WSUS console can't connect, it likely indicates a problem with either trusting the certificate, name resolution, or the port being blocked.

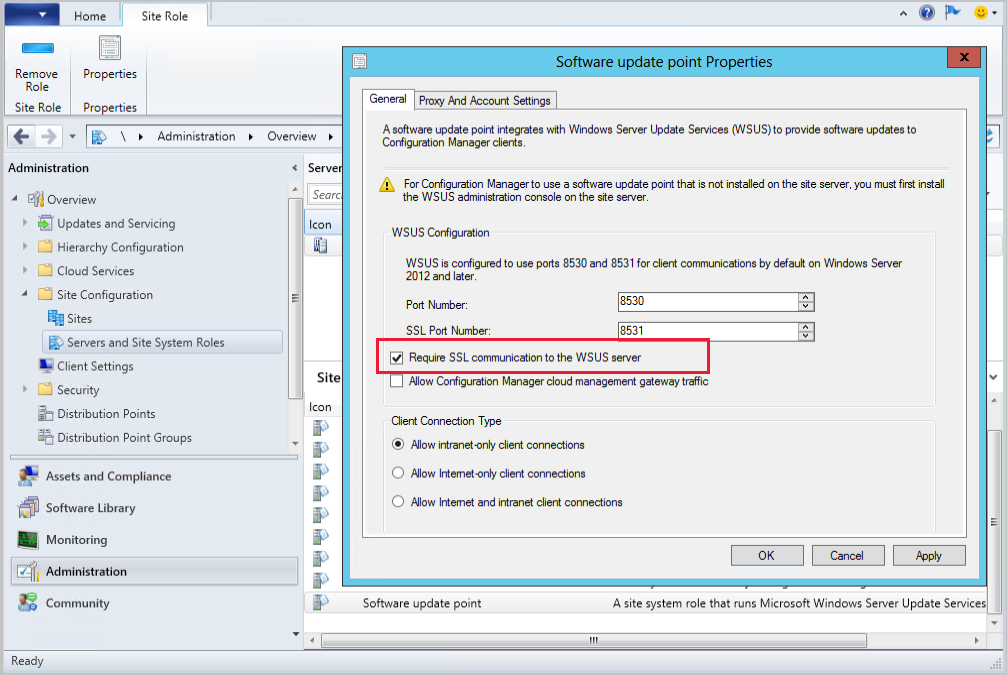
**Configure the software update point to require SSL communication to the WSUS server**

Once WSUS is set up to use TLS/SSL, you'll need to update the corresponding Configuration Manager software update point to require SSL too. When you make this change, Configuration Manager will:

* Verify it can configure the WSUS server for the software update point
* Direct clients to use the SSL port when they're told to scan against this WSUS server.

To configure the software update point to require SSL communication to the WSUS server, do the following steps:

1. Open the Configuration Manager console and connect to either your central administration site or the primary site server for the software update point you need to edit.
2. Go to **Administration** > **Overview** > **Site Configuration** > **Servers and Site System Roles**.
3. Select the site system server where WSUS is installed, then select the software update point site system role.
4. From the ribbon, choose **Properties**.
5. Enable the **Require SSL communication to the WSUS server** option.



1. In the [**WCM.log**](https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/log-files#BKMK_SUPLog) for the site, you'll see the following entries when you apply the change:

**WSUS Cleanup Task and Synchronization**

In SCCM, you can manage WSUS and Office 365 updates through Software Update Point and ADR configurations. For WSUS, use the "Run WSUS cleanup wizard" option within the Software Update Point settings to optimize the WSUS database. For Office 365 updates, enable Configuration Manager's ability to manage them and create ADRs to deploy them to target collections. Multiple ADR deployments can be managed with careful scheduling and target collection configuration

1. **Enable WSUS Cleanup Wizard:** In the Configuration Manager console, navigate to Administration > Overview > Site Configuration > Sites. Select the top-level site and then configure the Software Update Point. In the "Supersedence Rules" tab, select "Run WSUS cleanup wizard" or "Run WSUS cleanup after synchronization" (depending on your SCCM version).
2. **Configure Synchronization:** Set the synchronization schedule (e.g., daily or weekly) and choose the time that minimizes network load and conflicts with other processes.
3. **Consider Upstream Servers:** If you have a hierarchy, configure WSUS servers at each tier to synchronize with the top-tier WSUS server.
4. **Reindexing:** After synchronization, consider reindexing the WSUS database on each WSUS computer for optimal performance.

**Office 365 Updates:**

1. **Enable Configuration Manager Management:** Configure the necessary settings in Microsoft 365 Apps documentation.
2. **Create ADRs:** Once you've enabled Configuration Manager to manage Office updates, create ADRs to deploy them to target collections.
3. **Configure Update Channel:** Configure the update channel (e.g., Validation, First Release, Deferred) in the GPO for Office 365 clients.
4. **Testing and Validation:** Thoroughly test ADR deployments in a test environment before deploying them to production.

**Multiple ADR Deployments:**

1. **Schedule ADRs Carefully:** Ensure ADRs are scheduled to complete synchronization before they run, preventing conflicts.
2. **Use Targeted Collections:** Use specific collections for ADR deployments to avoid unnecessary deployments.
3. **Deployment Packages:** Create deployment packages to store update content and distribute it to distribution points.
4. **Monitor and Troubleshoot:** Monitor ADR deployments and troubleshoot any issues that may arise.

**How to use Software Metering in SCCM to track application usage:**

**In SCCM, Software Metering enables tracking of application usage, providing insights into software usage patterns and helping to optimize software licensing and deployment. It monitors Windows desktop applications (with .exe extensions) and reports usage data back to the SCCM server**

1. ***Enable Software Metering*: In the SCCM console, navigate to Administration > Client Settings > Default Client Settings, and enable software metering.**
2. ***Create Software Metering Rules*: Define rules that specify which applications to monitor. These rules can be based on executable file names (.exe) or MSI product codes.**
3. ***Deploy Configuration Baseline*: If necessary, deploy a configuration baseline that includes the software metering settings to the target devices.**
4. ***Monitor Software Usage*: SCCM will automatically collect and report usage data, which can be viewed in reports or by querying the database.**
5. ***Analyze and Optimize*: Analyze the collected data to identify trends and make informed decisions about software licensing, deployment, and procurement.**

**Additional details:**

* **Software Metering collects data separately from hardware or software inventory cycles.**
* **The data collection frequency can be configured, with a default setting of once every 7 days.**
* **Software Metering primarily focuses on Windows desktop applications (.exe files) and doesn't monitor modern Windows applications (like those used by Windows 8).**
* **You can use PowerShell cmdlets like New-CMSoftwareMeteringRule to automate the creation of metering rules.**
* **The SCCM console provides reports and views that display software metering information.**
* **Software metering data can be used to optimize software licensing, reduce licensing costs, and ensure compliance with software usage agreements**

**Managing Software Updates:**

In **Configuration Manager**, you can manage software updates by sorting, filtering, and searching the All Software Updates list. You can create Software Update Groups and Deployment Packages to organize and deploy updates to client computers

* ***Sorting:*** *The "All Software Updates" list can be sorted by various criteria, such as update name, severity, product, or deployment status.*
* ***Filtering:*** *You can filter the list to display specific updates based on criteria like severity, product, update type, or whether they are deployed or not.*
* ***Searching:*** *Use the search bar to find updates by name, bulletin ID, or other relevant keywords.*
* ***Software Update Groups:*** *Create groups to manage and deploy multiple updates together. You can define rules for automatically adding updates to groups or manually add them.*
* ***Deployment Packages:*** *Create packages to distribute the necessary update content to distribution points, which are then used to deploy updates to client computers.*

***Creating Software Update Groups:***

1. *Navigate to the Software Library workspace in the Configuration Manager console.*
2. *Select "All Software Updates".*
3. *Choose the updates you want to add to the group.*
4. *Click "Create Software Update Group" in the ribbon.*
5. *Provide a name and description for the group.*
6. *Click "Create".*

***Creating Deployment Packages:***

1. *Navigate to the Software Distribution area in the Configuration Manager console.*
2. *Right-click "Packages" and select "Distribute Software".*
3. *Follow the wizard to create a new package and specify the source location for the updates.*
4. *Associate the package with one or more distribution points.*

***Deployment Process:***

1. *The software updates are added to a software update group.*
2. *The software update group is deployed to a target collection of client computers.*
3. *The update policy is sent to the client computers, and the update content files are downloaded from a distribution point to the local cache.*
4. *The updates are then available for installation on the client computers.*

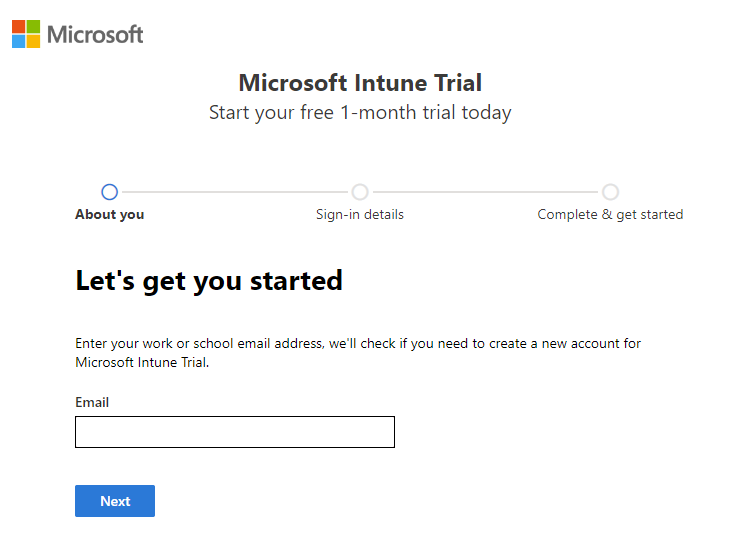
**MICROSOFT INTUNE**

Intune provides mobile device management (MDM) and mobile app management (MAM) from a secure cloud-based service that is administered using the Microsoft Intune admin center. Using Intune, you ensure your workforce's corporate resources (data, devices, and apps) are correctly configured, accessed, and updated, meeting your company's compliance policies and requirements.

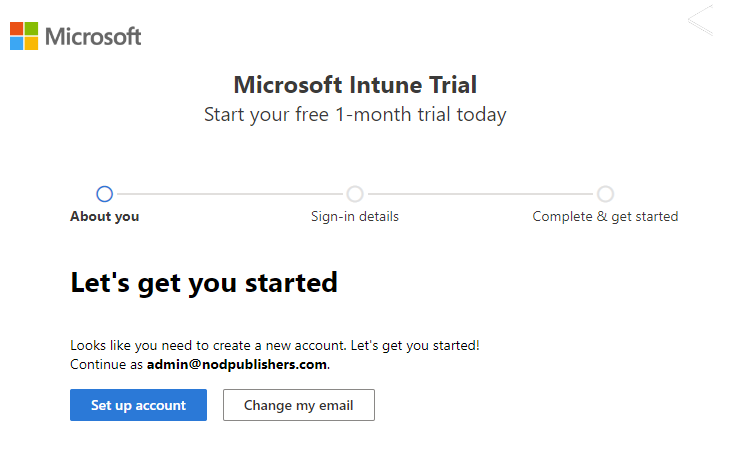
When you complete the signup process, you'll have a new tenant. A tenant is a dedicated instance of Microsoft Entra ID where your subscription to Intune is hosted. You can then configure the tenant, add users and groups, and assign licenses to users. When you're ready, you can help users enroll their devices and add apps that they need to begin the modern endpoint management process. As you continue, you can set configuration and protection policies, as well as other endpoint management capabilities.

To sign up for the Microsoft Intune free trial, follow the steps below:

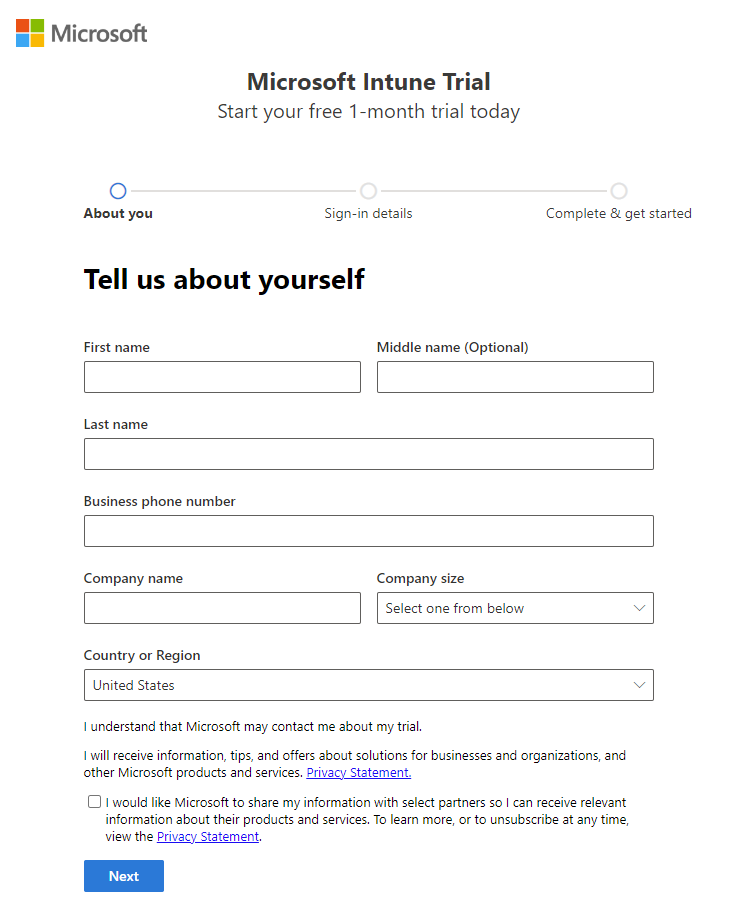
1. Navigate to the [Intune set up account page](https://go.microsoft.com/fwlink/?linkid=2019088).
2. Enter your email address and click **Next**.



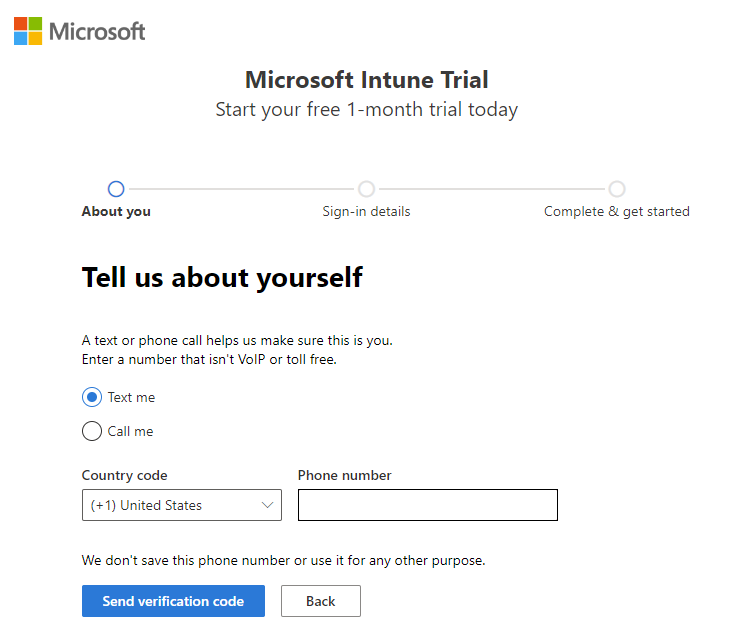
1. Click **Set up account** to create a new account.



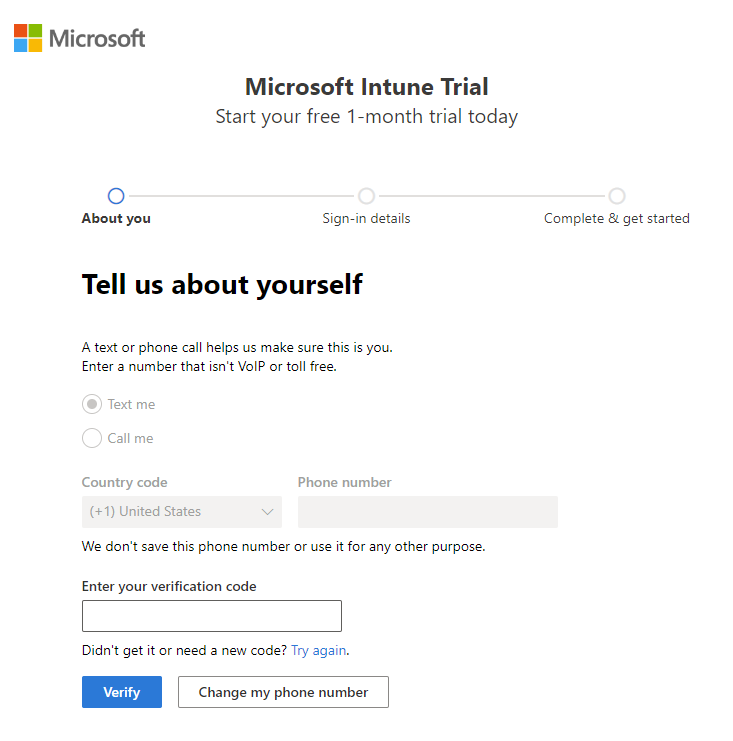
1. Add your name, phone number, company name, company size, and region. Review the remaining information and click **Next**.



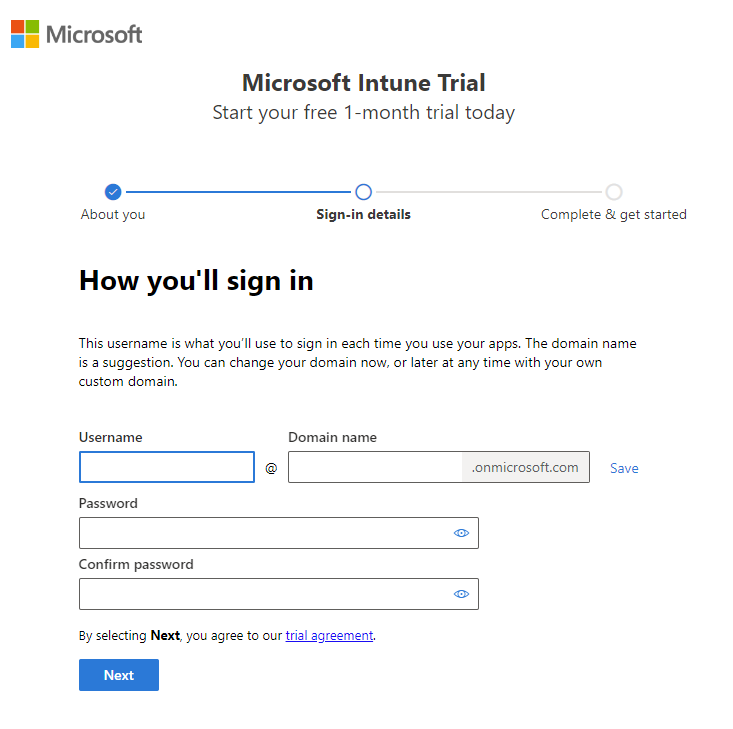
1. Click **Send verification code** to verify the phone number you added.



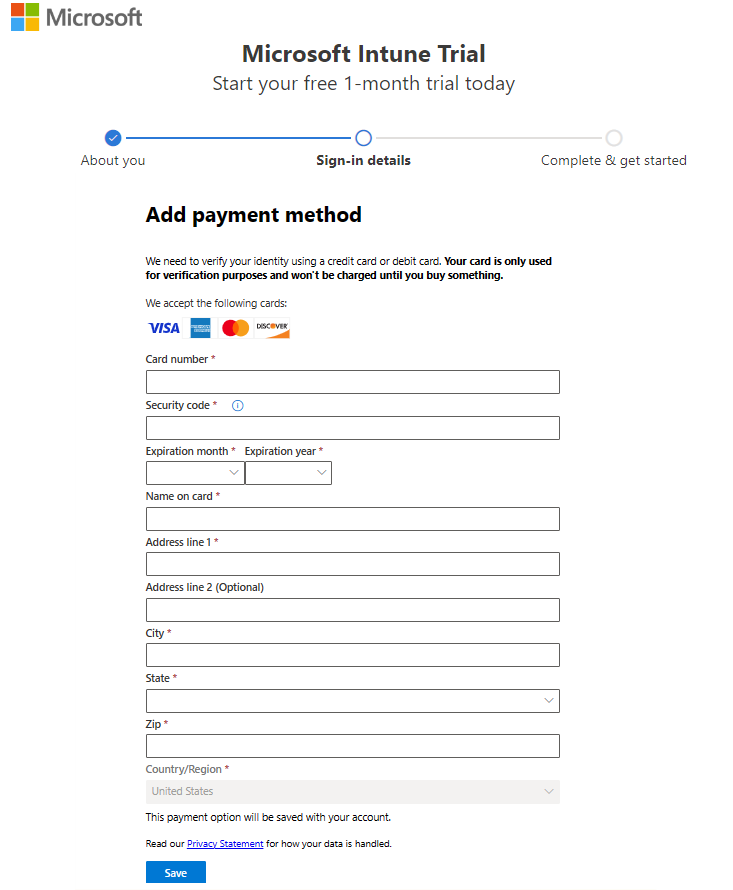
1. Enter the verification code you receive on your mobile device, then click **Verify**.



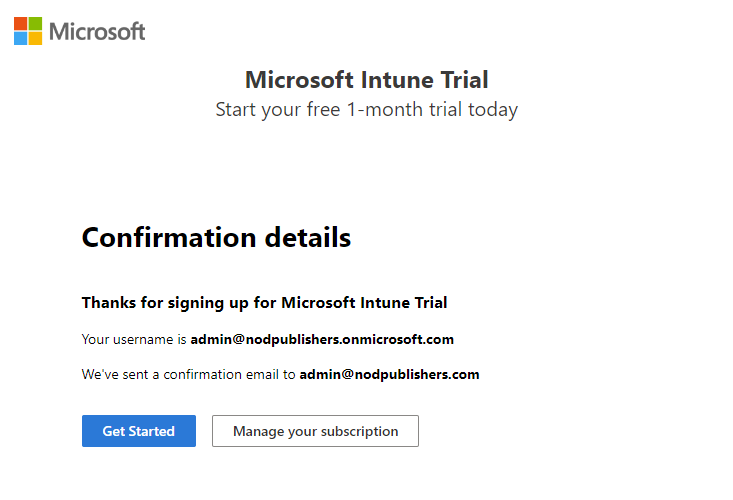
1. Add your **Username** and **Domain name** for your trial that represents your business or organization. Your name will be added before *.onmicrosoft.com*. Click **Save** to check availability. Click **Next** to continue. If you like, you can later change this domain name to your custom domain name.



1. In order to verify your identity, you must add a payment method. Your card is only used for verification purposes and won't be charged until you buy something.



1. After your account has been created, you'll see your user name. You'll use this user name to log in to Intune. Additionally, you receive an email message that contains your account information at the email address that you provided during the sign-up process. This email confirms your subscription is active.



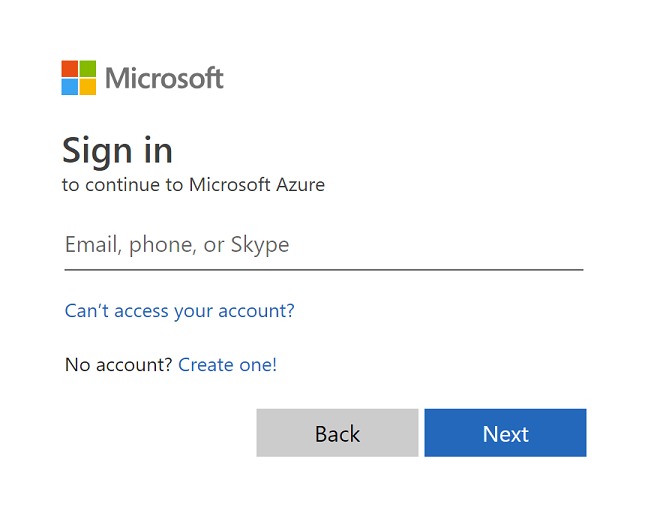
**Note**

If you click **Get Started**, you'll open the **Microsoft 365 admin center** home page. If you click **Manage your subscription**, you'll open **Your products** and view details about your Microsoft Intune Trial subscription.

**Sign in to Intune in the Microsoft Intune admin center**

If you're not already signed in to the admin center, complete the following steps:

1. Open a new browser window and enter [**https://intune.microsoft.com**](https://intune.microsoft.com/) in the address bar.
2. Use the user ID that you were given in the steps above to sign in. The user ID will look similar to the following: *yourID@yourdomain.onmicrosoft.com*.



**What is Client Cache Setting in SCCM**

The client cache stores temporary files for when clients install applications and programs. Software updates also use the client cache, but always attempt to download to the cache whatever of the size setting. Configure the cache settings, such as size and location, when you manually install the client, when you use client push installation, or after installation.

The Configuration Manager client downloads the content for required software soon after the deployment's available time but waits to run it until the deployment's scheduled time. At the scheduled time, the Configuration Manager client checks to see whether the content is available in the cache. If content is in the cache and it's the correct version, the client uses the cached content. When the required version of the content changes, or if the client deletes the content to make room for another package, the client downloads the content to the cache again.

If the client attempts to download content for a program or application that's greater than the size of the cache, the deployment fails because of insufficient cache size. The client generates status message 10050 for insufficient cache size. If you increase the cache size later, the result is:

* For a required program: The client doesn't automatically retry to download the content. Redeploy the package and program to the client.
* For a required application: The client automatically retries to download the content when it downloads its client policy.

If the client attempts to download content that's less than the size of the cache, but the cache is full, all *required* deployments keep retrying until:

* The cache space is available
* The download times out
* The retry count reaches its limit

